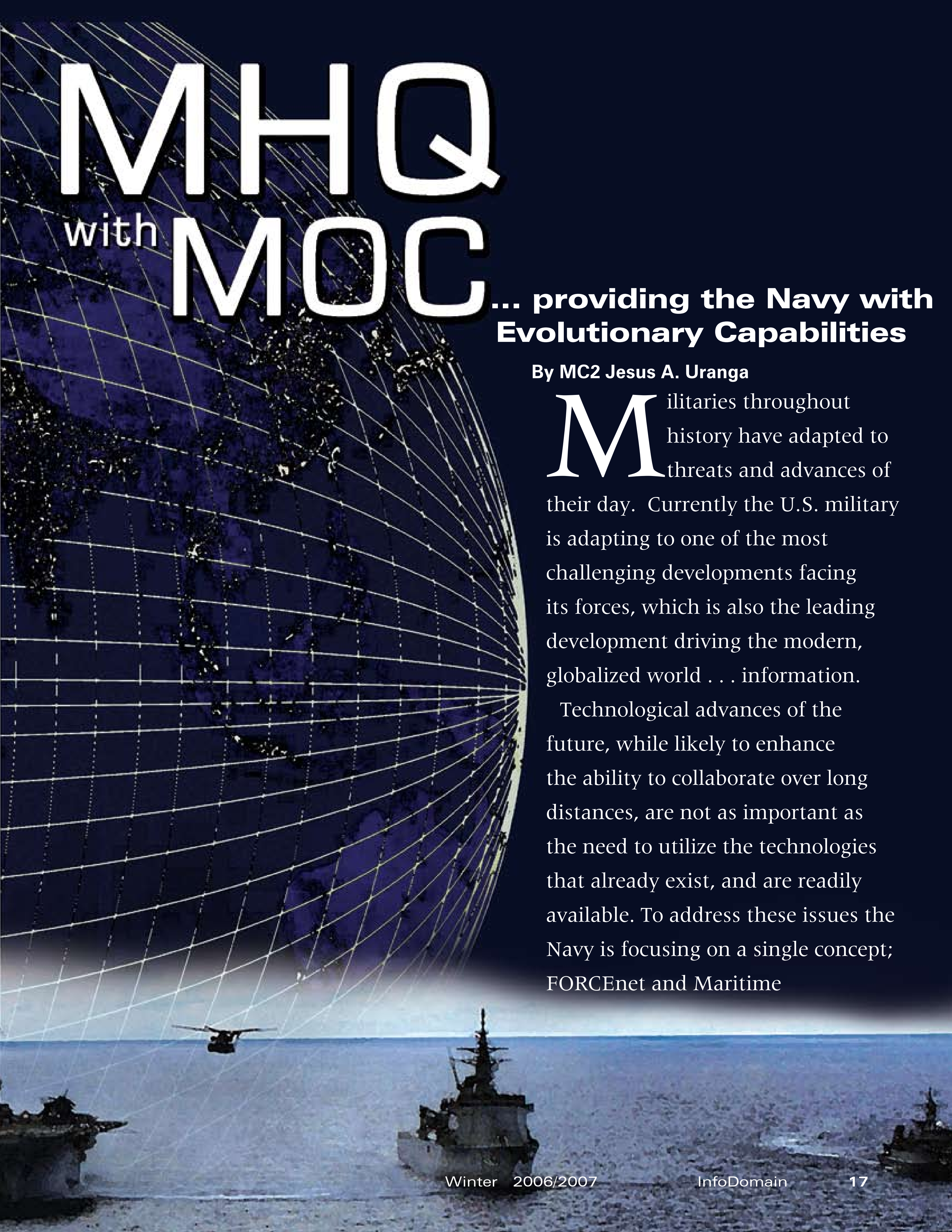

MHQ with MOC... providing the Navy with Evolutionary Capabilities

By MC2 Jesus A. Uranga

Militaries throughout history have adapted to threats and advances of their day. Currently the U.S. military is adapting to one of the most challenging developments facing its forces, which is also the leading development driving the modern, globalized world . . . information.

Technological advances of the future, while likely to enhance the ability to collaborate over long distances, are not as important as the need to utilize the technologies that already exist, and are readily available. To address these issues the Navy is focusing on a single concept; FORCEnet and Maritime

Continued from page 17

Heaquarters with Maritime Operations Centers.

FORCEnet is defined as the operational construct and architectural framework for naval warfare in the Information Age. It involves integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force.

The importance of powerful, reliable networks was recently accentuated, ironically not by a military conflict, but by the catastrophe brought on by Hurricane Katrina. The aftermath displayed on the world stage the need for greater communication and cooperation by all government and non-government agencies. The Navy has taken what it learned during Katrina and the current Global War on Terrorism and used that information in developing future concepts.

"FORCEnet is all about command and control and it is the driving force behind the MHQ with MOC concept of operations," said CAPT Rick Simon, NETWARCOM's FORCEnet director.

The overarching warfighting capabilities required by National, DoD, and Navy strategies and the 2006 Quadrennial Defense Review enjoins services to make rapidly deployable headquarters capability available to meet all contingencies.

The MHQ with MOC CONOPS is focused on providing methods by which different MHQ staffs may evolve toward standardization of assessment, planning, and execution at the operational level of war. It recommends changes to existing operational command processes and methods used by numbered fleet commanders, principal headquarters commanders, and the seven Navy component commanders while continuing to support fleet management.

The MOC is a distinct, functionally organized element of the MHQ, which conducts service and joint operations as required by the MHQ commander. The term MOC is inclusive of those personnel, processes, methods, and systems needed to support operations. Intelligence and logistics capabilities will be fully integrated in the MOC to enable and enhance the MHQ's ability to assess, plan, and execute operational level missions, including strategic communications, theater security cooperation, intelligent preparation of the environment, and maritime security operations.

The MOC is scalable to increase capacity as needed depending on the complexity and scope of operations to meet the requirements of the Joint Force Commander. For missions of increased scope and complexity, the MOC would be augmented as required with additional systems, processes, and personnel (Navy, Joint, allied, coalition, or interagency) tailored to meet mission requirements.

Implementation of these concepts is an ongoing evolution, and full integration into the fleet is presently in a spiral development stage. Currently, MHQ with MOC is a concept directly derived from the FORCEnet concept and architecture. The concept is still being developed, and tested by the NetOps, Information Operations and Space Center in Norfolk. Presently, NIOSC is designated a functional MOC as it will provide NetOps, Information Operations and space support to MOCs.

Information Assurance**Tips**

Wireless Network Security Basics: WEP

As the use of wireless technology continues to expand, there are several key points to be aware of regarding wireless security and Wired Equivalent Privacy.

WEP is the encryption standard most often used when personal wireless networks are set up at home. WEP encrypts and decrypts the payload of each packet that is transmitted. The security problem is that WEP uses a weak encryption scheme and can be easily cracked using tools freely available on the Internet.

On average, the encryption key used by WEP can be cracked after collecting packets from any wireless network for only a few hours. Once the WEP encryption key has been cracked, the traffic can now be "sniffed" and collected for later playback and analysis. This means everything is vulnerable that is sent over the wireless network that relies only on WEP for security.